BÁO CÁO BÀI THỰC HÀNH SỐ 4

PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG DoS

***Sinh viên 1:***

***Sinh viên 2:***

***Yêu cầu kết quả thực hành:***

Đóng gói các kết quả vào file nén có tên theo định dạng NhomX\_Lab04\_BaoCao.zip. Kết quả bao gồm có:

* Báo cáo kết quả thực hành
* File mã nguồn tấn công kịch bản 4

**KẾT QUẢ THỰC HÀNH**

1. **Kịch bản 1 (3 điểm)**

***Không có hình ảnh minh chứng: không có điểm cho mục tương ứng***

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trong khi bị tấn công: ***0.5 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trong khi bị tấn công: ***0.5 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích đặc điểm lưu lượng bằng Wireshark trên máy nạn nhân khi bị tấn công ***(1 điểm)***

*Trả lời:*

*<(Các)Ảnh chụp hình ảnh lưu lượng minh chứng cho nhận xét>*

* Tên của kỹ thuật DoS trong kịch bản này là gì? ***(0.25 điểm)***

*Trả lời:*

* Hậu quả của tấn công trên máy nạn nhân là gì? ***(0.25 điểm)***

*Trả lời:*

*Nếu nhận xét không phù hợp với phân tích kết quả lệnh top, iftop thì không có điểm phần này.*

1. **Kịch bản 2 *(3 điểm)***

***Không có hình ảnh minh chứng: không có điểm cho mục tương ứng***

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trong khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trong khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích đặc điểm lưu lượng bằng Wireshark trên máy nạn nhân khi bị tấn công ***(1 điểm)***

*Trả lời:*

*<(Các)Ảnh chụp hình ảnh lưu lượng minh chứng cho nhận xét>*

* Tên của kỹ thuật DoS trong kịch bản này là gì? ***(0.25 điểm)***

*Trả lời:*

* Hậu quả của tấn công trên máy nạn nhân là gì? ***(0.25 điểm)***

*Trả lời:*

*Nếu nhận xét không phù hợp với phân tích kết quả lệnh top, iftop thì không có điểm phần này.*

* Mô tả ngắn gọn cách thức phòng chống dạng tấn công này?***(0.5 điểm)***

*Trả lời:*

*Nếu liệt kê thêm các giải pháp khác mà không có căn cứ giải thích rõ ràng thì trừ 0.25 điểm*

1. **Kịch bản 3 *(4 điểm)***

***Không có hình ảnh minh chứng: không có điểm cho mục tương ứng***

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trước khi bị tấn công: ***0.25 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích lệnh kết quả thực hiện lệnh **top** và cho biết mức tiêu thụ tài nguyên CPU và RAM trên máy chủ nạn nhân trong khi bị tấn công: ***0.5 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh top>*

* Phân tích kết quả thực hiện lệnh **iftop** và cho biết lượng lưu lượng mà máy chủ nạn nhân phải nhận trong khi bị tấn công: ***0.5 điểm***

*Trả lời:*

*<Ảnh chụp kết quả thực hiện lệnh iftop>*

* Phân tích đặc điểm lưu lượng bằng Wireshark trên máy nạn nhân khi bị tấn công ***(1.5 điểm)***

*Trả lời:*

*<(Các)Ảnh chụp hình ảnh lưu lượng minh chứng cho nhận xét>*

* Tên của kỹ thuật DoS trong kịch bản này là gì? ***(0.25 điểm)***

*Trả lời:*

* Hậu quả của tấn công trên máy nạn nhân là gì? ***(0.25 điểm)***

*Trả lời:*

*Nếu nhận xét không phù hợp với phân tích kết quả lệnh top, iftop thì không có điểm phần này.*

* Mô tả ngắn gọn cách thức phòng chống dạng tấn công này?***(0.5 điểm)***

*Trả lời:*

*Nếu liệt kê thêm các giải pháp khác mà không có căn cứ giải thích rõ ràng thì trừ 0.25 điểm*